UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/825,596	04/14/2004	Cheh Goh	B-5414 621818-0	7793

22879 7590 07/21/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
GERGISO, TECHANE	

ART UNIT	PAPER NUMBER
2137	

NOTIFICATION DATE	DELIVERY MODE
07/21/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/825,596	GOH ET AL.	
	Examiner	Art Unit	
	TECHANE J. GERGISO	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04/18/2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *23-28 and 43-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *23-28 and 43-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04/14/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a non-Final Office Action in response to the applicant's communication filed on April, 18, 2008.

2. Claim 23-28 and 43-58 have been examined and are pending.

Election/Restrictions

3. Applicant's election without traverse of group II, namely claims 23-28 and 43-58 in the reply filed on April 18, 2008 is acknowledged.

4. Claims 1-22 and 29-42 withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected group I, namely claims 1-22 and claims 29-42, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on April 18, 2008

Claim Objections

5. Claims 23, 28, 43 and 48-58 are objected to because of the following informalities: All occurrences of "**organisation**" in claims 23, 28 43 and 48-58 have spelling or typo errors and need to be replaced with "**organization**". Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 23-28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Limitations of claims 23-28 are not positively recited in active steps and therefore the claims are rendered ambiguous and indefinite to precisely define the boundary and scope of the claims.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 23-28 and n43-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Appenzeller et al (Hereinafter referred to as, Appenzeller, US Pub No.: 2004/0098589 A1) in view Boneh et al. (hereinafter referred to as Boneh, US Pub No.: 2003/0081785 A1).

As per claim 23:

Appenzeller discloses a secure data-provision method comprising providing target data from a data provider to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organization, the target data being provided in encrypted form as part of a data set that comprises:

a first item encrypted, according to an Identifier-Based Encryption, IBE, scheme, in dependence on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority (0047; 0070; 0076; 0079); and

a second item encrypted according to an IBE scheme, in dependence on encryption parameters comprising a second encryption key string that identifies said specific organization, and public data of a second trusted authority (0047; 0070; 0076; 0079);

recovery of the target data in clear requiring decryption of both the first and second items (0058; 0068).

Appenzeller does not explicitly disclose a first trusted authority competent in respect of professional accreditations and a second trusted authority competent in respect of accreditations of organizations. Boneh, in analogous art, however discloses a first trusted authority competent in respect of professional accreditations and a second trusted authority competent in respect of accreditations of organizations (0053; 0054). Therefore, it could have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Appenzeller to include a first trusted authority competent in respect of professional accreditations and a second trusted authority competent in respect of accreditations of organizations. This modification could have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a system of encrypting a first piece of information to be sent by a sender to a receiver uses an encryption key generated from a second

piece of information using a bilinear map and the encryption key are used to encrypt at least a portion of the first piece of information to be sent from the sender to the receiver. The bilinear map may be symmetric or asymmetric as suggested by Boneh in (0110).

As per claim 24:

Appenzeller discloses a method, wherein the first item comprises the target data, and the second item comprises the encrypted first item (0047).

As per claim 25:

Appenzeller discloses a method, wherein the first item comprises the target data, and the second item comprises a nonce; the first encryption key string comprising, in combination, an identifier of said specific individual and said nonce (0020; 0047; 0079).

As per claim 26:

Boneh discloses a method, wherein the first item comprises first data, and the second item comprises second data; the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data (0010; 0050).

As per claim 27:

Boneh discloses a method, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising

a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key (0010; 0050).

As per claim 28:

Appenzeller discloses a secure data-provision method comprising providing target data from a data provider to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organization, the target data being provided in encrypted form as part of a data set that comprises:

a first item encrypted using both a first encryption key string that identifies said specific individual, and public data of a first trusted authority (0047; 0070; 0076; 0079); and

a second item encrypted using both a second encryption key string that identifies said specific organization, and public data of a second trusted authority (0047; 0070; 0076; 0079);

recovery of the target data in clear requiring decryption of both the first and second items (0058; 0068).

Appenzeller does not explicitly disclose a first trusted authority competent in respect of professional accreditations and a second trusted authority competent in respect of accreditations of organizations. Bonch, in analogous art, however discloses a first trusted authority competent in respect of professional accreditations and a second trusted authority competent in respect of accreditations of organizations (0053; 0054). Therefore, it could have been obvious to a person

having ordinary skill in the art at the time the invention was made to modify the system disclosed by Appenzeller to include a first trusted authority competent in respect of professional accreditations and a second trusted authority competent in respect of accreditations of organizations. This modification could have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a system of encrypting a first piece of information to be sent by a sender to a receiver uses an encryption key generated from a second piece of information using a bilinear map and the encryption key are used to encrypt at least a portion of the first piece of information to be sent from the sender to the receiver. The bilinear map may be symmetric or asymmetric as suggested by Boneh in (0110).

As per claim 43:

Appenzeller discloses an apparatus for the secure provision of target data to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organization, the apparatus comprising an encryption subsystem for generating a data set including the target data in encrypted form, the encryption subsystem comprising:

first encryption means for encrypting a first item, according to an Identifier-Based Encryption, IBE, scheme, based on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority (0047; 0070; 0076; 0079);

second encryption means for encrypting a second item, according to an IBE scheme, based on encryption parameters comprising a second encryption key string that

identifies said specific organization, and public data of a second trusted authority (0047; 0070; 0076; 0079); and

means for forming the data set using at least the encrypted first and second items; the recovery of the target data in clear requiring decryption of both the first and second items (0058; 0068).

Appenzeller does not explicitly disclose a first trusted authority competent in respect of professional accreditations and a second trusted authority competent in respect of accreditations of organizations. Boneh, in analogous art, however discloses a first trusted authority competent in respect of professional accreditations and a second trusted authority competent in respect of accreditations of organizations (0053; 0054). Therefore, it could have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Appenzeller to include a first trusted authority competent in respect of professional accreditations and a second trusted authority competent in respect of accreditations of organizations. This modification could have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a system of encrypting a first piece of information to be sent by a sender to a receiver uses an encryption key generated from a second piece of information using a bilinear map and the encryption key are used to encrypt at least a portion of the first piece of information to be sent from the sender to the receiver. The bilinear map may be symmetric or asymmetric as suggested by Boneh in (0110).

As per claim 44:

Appenzeller discloses an apparatus, wherein the first item comprises the target data, and the second item comprises the encrypted first item (0047).

As per claim 45:

Appenzeller discloses an apparatus, wherein the first item comprises the target data, and the second item comprises a nonce; the first encryption key string comprising, in combination, an identifier of said specific individual and said nonce (0020; 0047; 0079).

As per claim 46:

Appenzeller discloses an apparatus, wherein the first item comprises first data, and the second item comprises second data; the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data (0010; 0050).

As per claim 47:

Appenzeller discloses an apparatus, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key (0010; 0050).

As per claim 48:

Appenzeller discloses a computing entity for recovering target data provided in encrypted form as part of an data set that comprises first and second encrypted items both of which must be

decrypted to recover the target data, the first item being encrypted in dependence on encryption parameters comprising a first encryption key string that identifies a specific individual and first public data, and the second item being encrypted in dependence on a second encryption key string that identifies a specific organization and second public data; the entity comprising:

first means for requesting either a first decryption key corresponding to the first encryption key string, or the first item in decrypted form, from a first trusted authority and holds first private data related to the first public data, the first means being arranged to provide the first encryption key string to the first trusted authority when making its request and being further arranged to authenticate the entity with the first trusted authority and to receive the first decryption key, or the first item, securely from the first trusted authority (0047; 0070; 0076; 0079);

second means for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, which holds second private data related to the second public data, the second means being arranged to provide the second encryption key string to the organization when making its request and being further arranged to authenticate the entity with the organization and receive the second decryption key, or the second item, from the organization (0047; 0070; 0076; 0079);

third means for using the first decryption key, or the first item, provided by the first trusted authority and the second decryption key, or the second item, provided by the organization, to recover the target data (0058; 0068).

Appenzeller does not explicitly disclose an organization accredited by a second trusted authority. Boneh, in analogous art, however discloses an organization accredited by a second trusted authority (0053; 0054). Therefore, it could have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Appenzeller to include an organization accredited by a second trusted authority. This modification could have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a system of encrypting a first piece of information to be sent by a sender to a receiver uses an encryption key generated from a second piece of information using a bilinear map and the encryption key are used to encrypt at least a portion of the first piece of information to be sent from the sender to the receiver. The bilinear map may be symmetric or asymmetric as suggested by Boneh in (0110).

As per claim 49:

Appenzeller discloses a computing entity, wherein the second means is arranged to receive the second decryption key, or the second item, securely from the organization (0047).

As per claim 50:

Appenzeller discloses a computing entity, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the third means being arranged to:recover the second item, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization, and subject the

second item to decryption, using the first decryption key obtained from the first trusted authority, to recover the target data (0077; 0082).

As per claim 51:

Boneh discloses a computing entity, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the third means being arranged to:

recover the second item, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization (0022-0025),

combine the nonce that formed the second item with the identifier of said specific individual in order to form the first encryption key string to be provided by the first means to the first trusted authority (0024, 0040; 0043), and

use the first decryption key obtained from the first trusted authority to decrypt the first item and thereby recover the target data (0043).

As per claim 52:

Boneh discloses a computing entity, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the third means being arranged to

recover the first data, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority (0022-0025; 0043),

recover the second data, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization (0024, 0040; 0043),

use the first data and the second data to form said symmetric key, and use the symmetric key to decrypt the target data (0043).

As per claim 53:

Boneh discloses a computing entity, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the third means being arranged to:

recover the first item, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority (0022-0025; 0043),

recover the second item, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization (0024, 0040; 0043),

use the second symmetric key that formed the second item to decrypt the encrypted first symmetric key that formed the first item (0040; 0050) , and

use the first symmetric key to decrypt the encrypted target data (0040; 0050).

As per claim 54:

Boneh discloses a computing entity for recovering target data provided in encrypted form as part of an data set that comprises first and second encrypted items both of which must be decrypted to recover the target data; the first item being encrypted in dependence on a first encryption key string that identifies a specific individual, and first public data; and the second item being encrypted in dependence on a second encryption key that identifies a specific organization and said specific individual, and second public data; the entity comprising:

first means for requesting either a first decryption key corresponding to the first encryption key, or the first item in decrypted form, and holds first private data related to the first public data, the first means being arranged to provide the first encryption key string, or the first item, to the first trusted authority when making its request (0047; 0070; 0076; 0079);

second means for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, from an organization accredited by a second trusted authority which holds second private data related to the second public data, the second means being arranged to provide the second encryption key string to the organization when making its request (0047; 0070; 0076; 0079); and

third means for using the first decryption key, or the first item, provided by the first trusted authority and the second decryption key, or the second item, provided by the organization, to recover the target data (0058; 0068);

at least one of the first means and the second means being arranged to authenticate the entity to the first trusted authority or said organization as the case may be and to receive input therefrom in a secure manner (0058; 0068).

Appenzeller does not explicitly disclose a first trusted authority which is competent in respect of the accreditation of professionals. Boneh, in analogous art, however discloses a first trusted authority which is competent in respect of the accreditation of professionals (0053; 0054). Therefore, it could have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Appenzeller to include a first trusted authority which is competent in respect of the accreditation of professionals. This modification could have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a system of encrypting a first piece of information to be sent by a sender to a receiver uses an encryption key generated from a second piece of information using a bilinear map and the encryption key are used to encrypt at least a portion of the first piece of information to be sent from the sender to the receiver. The bilinear map may be symmetric or asymmetric as suggested by Boneh in (0110).

As per claim 55:

Appenzeller discloses a computing entity, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the third means being arranged to: recover the second item, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization, and subject the second item to decryption, using the first decryption key obtained from the first trusted authority, to recover the target data (0077; 0082).

As per claim 56:

Boneh discloses a computing, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the third means being arranged to:

recover the second item, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization (0022-0025),

combine the nonce that formed the second item with the identifier of said specific individual in order to form the first encryption key string to be provided by the first means to the first trusted authority (0024, 0040; 0043), and

use the first decryption key obtained from the first trusted authority to decrypt the first item and thereby recover the target data (0043).

As per claim 57:

Boneh discloses a computing entity, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the third means being arranged to

recover the first data, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority (0022-0025; 0043),

recover the second data, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization (0024, 0040; 0043),

use the first data and the second data to form said symmetric key, and use the symmetric key to decrypt the target data (0043).

As per claim 58:

Boneh discloses a computing entity, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the third means being arranged to:

recover the first item, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority (0022-0025; 0043),

recover the second item, if not provided to the second means in decrypted form by the organization, by using the second decryption key obtained from the organization (0024, 0040; 0043),

use the second symmetric key that formed the second item to decrypt the encrypted first symmetric key that formed the first item (0040; 0050), and

use the first symmetric key to decrypt the encrypted target data (0040; 0050).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior art.

Contact Information

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is **(571) 273-3784**. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/T. J. G./

Examiner, Art Unit 2137

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2137